



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/432,007	11/01/1999	AKIHISA KAWASAKI	MAT-V07838	9503

7590 04/21/2005

LAWRENCE E ASHERY
RATNER & PRESTIA SUITE 301
ONE WESTLAKES BERWYN
PO BOX 980
VALLEY FORGE, PA 194820980

EXAMINER

ZIA, SYED

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/432,007

Applicant(s)

KAWASAKI, AKIHISA

Examiner

Syed Zia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 January 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6, 12 and 14 is/are rejected.
- 7) ☒ Claim(s) 7-11, 13, 15 and 16 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

47

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 24, 2005 has been entered.

Response to Amendment

This office action is in response to arguments filed on January 24, 2005. Original application contained Claims 1-28. Applicant previously amended Claim 1, 21-23, 25, 27 and 28. Applicant currently amended Claims 1, 12, and 14. Applicant currently cancelled claims 17-28. The amendment filed have been entered and made of record. Presently pending claims are 1-16.

Allowable Subject Matter

Claims 7-11, 13, and 15-16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

1.

Applicant's arguments filed on January 24, 2005 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claim 1 applicants argued that the cited admitted prior art (CPA) [Chaum et al.] does not teach, "*a system reproducing the individual user-end equipment secret information from the received individual user-end equipment information as set forth in claim*". This is not found persuasive. Cited prior art teaches system and method that is installed within a multi-lane toll plaza environment and has roadside collection stations (RCS) each of which communicates over a high speed short-range microwave or RF communication link with in vehicle units (IVU's). Each in-vehicle unit comprises an RF antenna having a pattern adapted for disposition in proximity to an associated vehicle and for communicating with a RCS while moving past it. RF circuits are connected to the antenna for operating in either a mode in which a data uplink is established with an RCS by modulating the reflectivity of the antenna or a mode in which a data downlink is established with an RCS by demodulating received RF signals. The IVU also includes a smart card controller removably connected with a smart card, and a link controller connected to the RF circuits and to the smart card controller. The link controller includes circuits for causing operation in the first mode to repetitively transmit first data to an RCS and in the second mode to receive second data, based at least in part on the first data, upon which operation is switched back to the first mode for transmission of third data based at least in

Art Unit: 2131

part on the second data, the first and third data together collectively comprising a cryptographically secured electronic money transfer.

As a result, Cited prior art does implement and teaches a system and method that provides an ETC authentication system and a method of the authentication, in which roadside equipment and central processing equipment are capable of making a direct authentication for legitimacy of an IC card (Fig.1-2, and 4-5).

5. Applicants have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2131

2. Claims 1-6, 12, and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Chaum et al. U. S. Patent (5,485,520).

3. Regarding Claim 1 Chaum teaches and describes an equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system (Fig.1), wherein;

- said user-end equipment provided with individual user-end equipment information issued by said key center and individual user-end equipment secret information corresponding to said individual user-end equipment's information, and said user-end equipment transmits said individual user-end equipment information to said system-end equipment (col.6 line 65 to col.7 line 65);

- said system-end equipment receives said individual user-end equipment information from said user-end equipment, reproduces by a system conversion said individual user-end equipment secret information from said received individual user-end equipment information using an equivalent secret key cryptographic algorithm of the key center, and authenticates said user-end equipment by confirming that said user-end equipment legitimately has said individual user-end equipment secret information by using a challenge response utilizing a common key cryptographic algorithm (col.7 line 38 to col.8 line 25); and

- said user-end equipment and said system-end equipment execute a cryptographic communication with each other using said individual user-end equipment secret information (col.9 line 36 to line 48).

Art Unit: 2131

4. Regarding Claim 12 Chaum teaches and describes an equipment authentication and cryptographic communication system, comprising: user-end equipment, system-end equipment, and a key center for administrating authentication of equipment in said system, wherein;

- said key center is provided with a first system converter for generating user-end equipment secret information from user-end equipment information (col.6 line 65 to col.7 line 7);

- said user-end equipment is provided with a first storage unit for storing said user-end equipment information provided by said key center, a second storage unit for storing said user-end equipment secret information, a first encryption unit, and a first decryption unit (col.7 line 37 to col.8 line 5, and col.10 line 66 to col.11 line 25); and

- said system-end equipment is provided with a second system converter for generating said user-end equipment secret information by a system conversion of said user-end equipment information received from said user-end equipment, a second encryption unit, and a second decryption unit said second system converter using an equivalent secret key cryptographic algorithm of the first system converter to generate said user-end equipment secret information from said received user-end equipment information, and wherein said user-end equipment and said system-end equipment share and utilize said user-end equipment secret information as a common key for-encryption and decryption in said first encryption unit and said first decryption unit in said user-end equipment, and said second encryption unit and said second decryption unit in said system-end equipment (col.9 line 25 to line 48).

Art Unit: 2131

5. Regarding Claim 14 Chaum teaches and describes a method of equipment authentication and cryptographic communication for an equipment authentication and cryptographic communication system including user-end equipment, system-end equipment, and a key center for administering authentication of equipment in said system, said method comprising the steps of:

- generating user-end equipment secret information from user-end equipment information in said key center (col.6 line 65 to col.7 line 7);

- receiving said user-end equipment information and said user-end equipment secret information in said user-end equipment from said key center (col.7 line 37 to col.8 line 5);

- receiving said user-end equipment information from said user-end equipment, and generating said user-end equipment secret information from said user-end equipment information received in said system-end equipment *by* a system conversion using an equivalent secret key cryptographic algorithm of said key center, and using said user-end equipment secret information as a common key for encryption and decryption in both of said user-end equipment and said system-end equipment (col.9 line 25 to line 48, and col.10 line 66 to col.11 line 25).

6. Claim 2 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

- said system-end equipment is provided with system-end equipment secret information, which is identical to that possessed by said key center, and produces individual user-end equipment secret information from said individual user-end equipment information using said system-end equipment secret information; and said user-end equipment authenticates said

Art Unit: 2131

system-end equipment by confirming that said system-end equipment has said individual user-end equipment secret information by a challenge response utilizing said common key cryptographic algorithm (col.15 line 65 to col.16 line 65).

7. Claim 3 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

- said system-end equipment is provided with a secret-key cryptographic algorithm, and reproduces said individual user-end equipment secret information by a system conversion of said individual user-end equipment information using a secret key (col.16 line 14 to col.16 line 65).

15. Claim 4 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein:

- said system-end equipment and said user-end equipment are both provided with common secret information shared there between by exchanging individually held secret information (col.16 line 14 to col.16 line 65).

16. Claim 5 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system wherein:

- said system-end equipment and said user-end equipment exchange with each other individually held secret information, and generate new secret information by combining said individually held secret information and said secret information exchanged there between according to a predetermined procedure (Col.15 line 22 to col.16 line 65).

17. Claim 6 is rejected applied as above rejecting Claim 1. Furthermore, Chaum teaches and describes equipment authentication and cryptographic communication system, wherein:

- said system-end equipment and said user-end equipment use said individual user-end equipment secret information for encrypting said new secret information, which is provided by combining said information and said exchanged information (col.16 line 32 to line 52).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


SZ

April 17, 2005